SIMON TOUCH

User Manual

ESL Tool

SIMON TOUCH

Overview

This software and accompanied drivers are intended for educational purposes only and it's use is sole liability of user. All further consequences of any other possible device use is subject of user's choice and responsibility.

The drivers, provided are original FTDI® files – both self-installing executable and zip archive, containing files for manual install. Choose the one suitable for You. Any further questions of misbehaved FTDI® drivers to be forwarded to their support center.

Hardware serial number is visible in Windows in “My Computer” / “Properties” / “Hardware” / “Device Manager” - selecting the device - “Properties” / “Details” / “Device Instance id” and Serial Number (8 digits and/or characters) is shown after VID and PID of the interface hardware. The method, described above may vary, depending on exact operation system You are using, but in general is the same. This unique serial number eases identification of Your hardware in manufacturer database, providing You corresponding initial software and further updates.

Hardware contains Lithium battery for backing up the critical data for supporting it's functionality. Do not use / store the device in extreme temperatures or inappropriate humidity or another operational conditions, as this could lead to big leakage currents, shortening battery life. Consult Lithium-battery specifications for proper storage and usage. In any case it is good idea to have device connected and powered by USB port or another external compatible +5V DC source for prolonging battery lifespan.

SIMON TOUCH

How to use

At start of the software, if hardware is properly connected, You will see the following (button/labels if not active, this means You did something wrong):

Always mind the exact order of connecting and disconnecting the ESL/interface/PC – not following might seriously harm any/all components:

1. Plug ESL Tool hardware to available USB port.
2. Connect ESL to ESL Tool hardware using it's fast installing 2-pin connector.
3. Power-on ESL from steady +12V DC power supply – it is a must!!!

Upon completion of Your work with ESL disconnect in the reverse order:

1. Power-off ESL by removing steady +12V DC power supply.
2. Disconnect ESL from ESL Tool hardware by removing 2-pin connector.
1. Unplug ESL Tool hardware from USB port of PC.

You could use ESL Tool for ESL units, which are not dismounted from car. Just be sure You have connected them properly to "GND" and "K-line" of ESL Tool hardware. Powering such units is a matter of choice – either use existing car +12V power supply or by external power unit. Power supply is very important for proper locking/unlocking of ESL – it might lead to undesirable effects if You can't guarantee proper power to the ESL. Consult vehicle's technical documentation for

available power supply connection point with enough current throughput.

Press “Read” button after selecting desired model of ESL:

After Hash data is read and shown on screen, be sure that You see all Keys Hashes, numbered from 1 to 8, preceded by so called “Service Hash” (also called “Dealer Password” or different, depending on people's habit to name it) and also data about software version of ESL should be present. All these Hashes records are needed for further comparison to data in EIS or Key or other modules – Electronic Control Unit (ECU) for the engine or transmission modules - “7G-Tronic” (ETC), ISM, etc... modules, which are related to FBS® (immobilizer) system.

The exact order of Hashes is very important and should be properly aligned to the corresponding data in Electronic Ignition Switch (EIS). If misaligned, the ESL unit will not unlock and not permit the EIS to turn into “Ignition ON” state or/and issue “Starter ON” signal. There are vast number of ESL stopped to operate due to corrupted Hashes. It is possible to operate (Lock / Unlock) the ESL with software, simulating presence of EIS, so misbehaving reason could be identified – EIS or ESL. Put the required Key Hash data – 8 bytes to the field “Hash / Dealer pass”, select Key number from the drop-down menu to it's right and press desired button - “Lock” or “Unlock”. Observe ESL operation and responses, presented by ESL Tool software – if ESL moves in desired position, then it's EIS fault, not sending it the needed data – check either EIS or “K-line” wiring between two modules. Consult technical documentation for wiring

diagrams of the vehicle model, being operated.

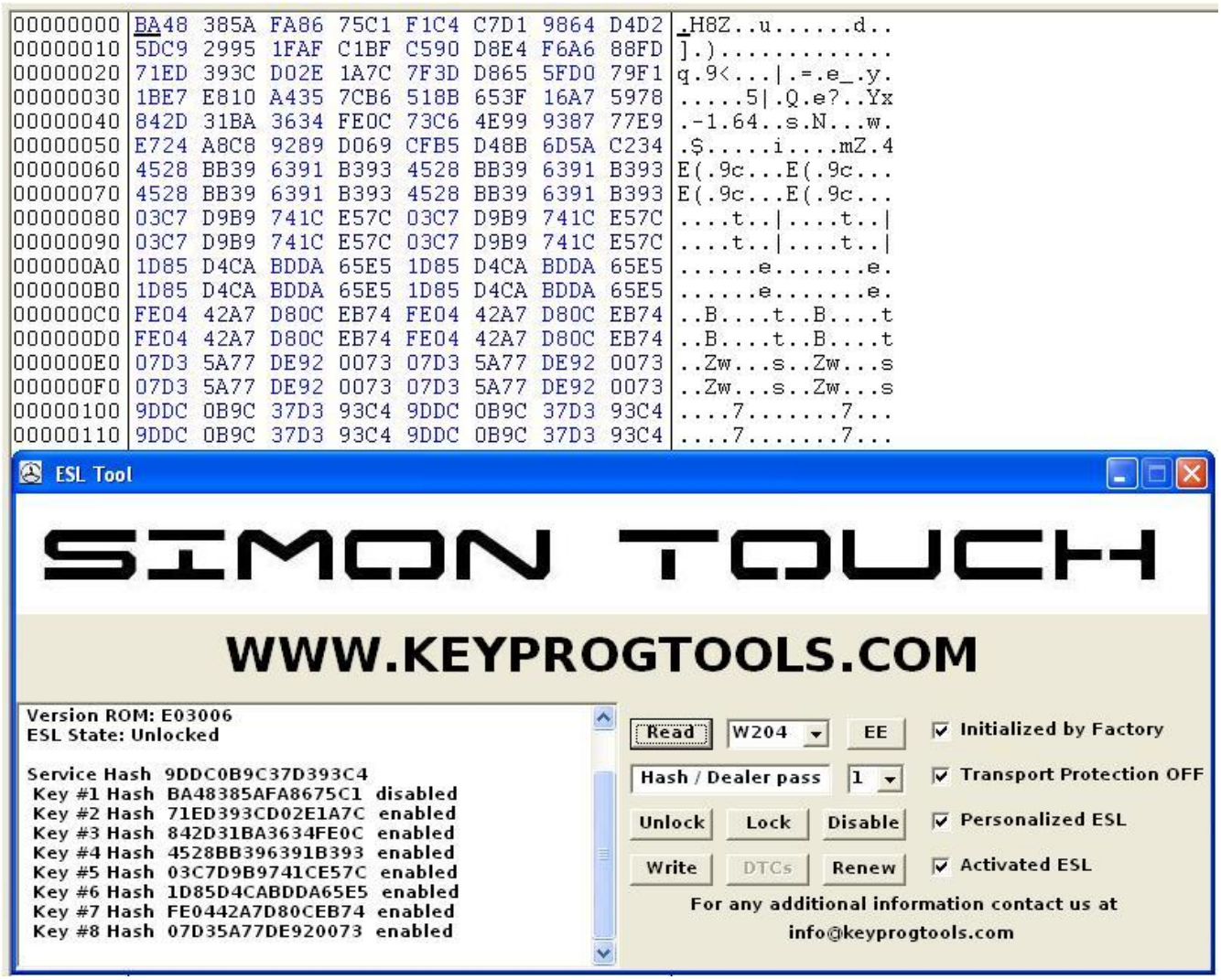
Always look the ESL State information, provided by software – if "Unlocked"/"Locked"/"Moving" or "Fault"! If internal position switches of ESL are faulty or got stuck by dirt or other reason, then ESL unit will not be able to follow properly it's movement and will not respond to EIS requests. It is very common for W204 ESL units. The unit could be in unlocked state with steering wheel free, while ESL reports "Moving" state. Dismantle the ESL and align it's moving parts to position switches, so correct information to be present. W204 motor's problems often cause it to stuck in the middle of it's movement, just before reaching end position, but enough to confuse position keys. Also after repairing / dismantling ESL it is important to put it in car with correct position – check it first with software, that it's properly assembled and not showing "Moving" before You connect it to car wiring.

If for some reason ESL unit is unrepairable, then You could put new ESL unit and adapt it to the car, using information, provided by us. Press "Write" button and select the file for the car, You are working on. The SSID, contained in file will be displayed and adaptation process will start:

When it is ready software will inform You and will put the ESL in "Locked" position. The adaptation process could be reversed by providing "Dealer pass" to the ESL – fill the 8 bytes data in field "Hash / Dealer pass" and click the button

"Renew". After successful completion of it, You could write ESL with new data.

In any moment You could check internal EEPROM content – either to see if adaptation runs OK or to get impression of hashes alignment, commented earlier. Click "EE" button and select a file name for the data to be read. You could use Your favorite binary editor/viewer to check the data read:


00000000 BA48 385A FA86 75C1 F1C4 C7D1 9864 D4D2 .H8Z..u.....d..
00000010 5DC9 2995 1FAF C1BF C590 D8E4 F6A6 88FD].).............
00000020 71ED 393C D02E 1A7C 7F3D D865 5FD0 79F1 q.9<...|.=.e_.y.
00000030 1BE7 E810 A435 7CB6 518B 653F 16A7 5978 .....5|.Q.e?..Yx
00000040 842D 31BA 3634 FE0C 73C6 4E99 9387 77E9 .-1.64..s.N...w.
00000050 E724 A8C8 9289 D069 CFB5 D48B 6D5A C234 .$.....i....mZ.4
00000060 4528 BB39 6391 B393 4528 BB39 6391 B393 E(.9c...E(.9c...
00000070 4528 BB39 6391 B393 4528 BB39 6391 B393 E(.9c...E(.9c...
00000080 03C7 D9B9 741C E57C 03C7 D9B9 741C E57C ....t..|....t..|
00000090 03C7 D9B9 741C E57C 03C7 D9B9 741C E57C ....t..|....t..|
000000A0 1D85 D4CA BDDA 65E5 1D85 D4CA BDDA 65E5 ......e.......e.
000000B0 1D85 D4CA BDDA 65E5 1D85 D4CA BDDA 65E5 ......e.......e.
000000C0 FE04 42A7 D80C EB74 FE04 42A7 D80C EB74 ..B....t..B....t
000000D0 FE04 42A7 D80C EB74 FE04 42A7 D80C EB74 ..B....t..B....t
000000E0 07D3 5A77 DE92 0073 07D3 5A77 DE92 0073 ..Zw...s..Zw...s
000000F0 07D3 5A77 DE92 0073 07D3 5A77 DE92 0073 ..Zw...s..Zw...s
00000100 9DDC 0B9C 37D3 93C4 9DDC 0B9C 37D3 93C4 ....7.......7...
00000110 9DDC 0B9C 37D3 93C4 9DDC 0B9C 37D3 93C4 ....7.......7...
ESL Tool
SIMON TOUCH
WWW.KEYPROGTOOLS.COM
Version ROM: E03006
ESL State: Unlocked
Service Hash 9DDC0B9C37D393C4
Key #1 Hash BA48385AFA8675C1 disabled
Key #2 Hash 71ED393CD02E1A7C enabled
Key #3 Hash 842D31BA3634FE0C enabled
Key #4 Hash 4528BB396391B393 enabled
Key #5 Hash 03C7D9B9741CE57C enabled
Key #6 Hash 1D85D4CABDDA65E5 enabled
Key #7 Hash FE0442A7D80CEB74 enabled
Key #8 Hash 07D35A77DE920073 enabled
Read
W204
EE
Initialized by Factory
Hash / Dealer pass
1
Transport Protection OFF
Unlock
Lock
Disable
Personalized ESL
Write
DTCs
Renew
Activated ESL
For any additional information contact us at
info@keyprogtools.com

Note, the given example is for W204 and every Key Hash has four consecutive records in EEPROM for Keys being used in car. For unused records data is just repeated. For W203 and older models it is presented different, containing just a half of every Hash record. Also note, that W204 ESL units has additional security features, involving not only Hashes data, but also a password,

which can not be read from the unit.

To complete the data in above noted files, You should use our NEC Key Tool ! Have in mind, that ESL Tool can't read ESL password, which is vital part of MB ® FBS immobilizer system and You can't use ESL Tool files for direct generation of new memory content for adapting it to car. Proceed further to NEC Key Tool User Manual to complete the process.

Important notice: There are new ESL units, that could be read only if they have "Transport Protection" removed. Others could be read even before adaptation process, but data they show is pre-programmed in factory and is for

test purposes only – it is not related to car being operated.